

**Review of the
Electronic Fraud Detection System**

June 1999

Reference Number: 093009

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.

Redaction Legend:

2b = Law Enforcement Guideline(s)
2e = Law Enforcement Procedure(s)



INSPECTOR GENERAL
for TAX
ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

June 2, 1999

MEMORANDUM FOR COMMISSIONER ROSSOTTI

David C. Williams

FROM:

David C. Williams
Inspector General

SUBJECT:

Final Audit Report – Review of the Electronic Fraud
Detection System

The attached report presents the results of our review of the Internal Revenue Service's (IRS) Electronic Fraud Detection System (EFDS). We conducted our review at the Ogden and Cincinnati Service Centers and the EFDS Project Office in Washington, DC, to determine if EFDS was functioning effectively and if the system was meeting proper control standards.

The report points out that while EFDS is a significant improvement over the manual procedures used prior to implementation of the system, there are still changes that can be made to further improve or better manage the system. The report discusses our concerns regarding security of the system, including control weaknesses that affect the system's security certification, delivery and effectiveness of some applications, and incomplete and inaccurate cost figures maintained by the Project Office.

Information Systems management has responded to the report and their comments are incorporated into the text where appropriate. In addition, the complete text of management's response is presented in Appendix V to the report. Information Systems management agreed with the findings in this report and has developed corrective actions to address the identified problems. We concur with the corrective actions outlined in management's response.

Copies of this report are also being sent to IRS managers who are affected by the report recommendations. Please call me at (202) 622-6500 if you have any questions, or your staff may contact Maurice S. Moody, Acting Assistant Inspector General for Audit at (202) 622-8500.

**Review of the
Electronic Fraud Detection System**

Table of Contents

Executive Summary	Page i
Objective and Scope	Page 1
Background	Page 1
Results.....	Page 2
Access Controls Should Be Improved.....	Page 4
The Electronic Fraud Detection System (EFDS) Application Audit Trail 2b, 2e-----	
2b, 2e-----	Page 9
The EFDS Application Audit Trail 2b, 2e-----	
2b, 2e-----	Page 13
EFDS Security Reviews at the Service Centers Are Not Being Performed	Page 18
Security Documentation Is Not Current and, in Some Instances, Does Not Reflect Current System Programming	Page 20
Contingency Plans Need to Be Updated and Tested	Page 22
EFDS Does Not Sort Cases to Ensure Returns With the Highest Potential for Fraud Are Reviewed First	Page 24
Some EFDS Applications Are Not Being Delivered Timely by Contract Developers	Page 25
Improvements Are Needed to Accurately Account for EFDS Costs	Page 28
Conclusion	Page 31
Appendix I - Detailed Objective, Scope and Methodology.....	Page 32
Appendix II - Major Contributors to This Report	Page 40
Appendix III - Report Distribution List.....	Page 41
Appendix IV - Response from Director of Investigations, Office of Refund Fraud, to Audit Memorandum	Page 42
Appendix V - Management's Response to the Draft Report.	Page 43
Appendix VI - Description of C2-Level Security.....	Page 63
Appendix VII - Glossary of Terms Used in This Report	Page 64

Review of the Electronic Fraud Detection System

Executive Summary

With the advent of electronic filing in 1986, the number of tax returns claiming fraudulent refunds has increased dramatically. As a result, the Internal Revenue Service (IRS) developed the Electronic Fraud Detection System (EFDS). At its inception, there were four basic goals for EFDS. These goals were to:

- Automate the labor-intensive manual screening process of the Questionable Refund Program.
- Improve techniques to identify returns with the highest potential for fraud, and ensure that these returns were reviewed.
- Increase data sources to improve detection of fraud.
- Enhance scheme development for referral to the districts for criminal prosecution.

We performed this review to determine if EFDS was meeting its program goals, objectives and proper control standards, and if the Project Office maintained reliable project cost data.

Results

The IRS has achieved many successes relative to its development of EFDS. Overall, EFDS has met most of its program goals and the needs of its users. The Project Office is working toward added functionality to help increase the Criminal Investigation Division's (CID) ability to detect fraudulent returns.

While the automated system is a significant improvement over the manual process used prior to EFDS, there are still changes that can be made to further improve or manage the system. We identified issues of concern regarding security of the system, delivery and effectiveness of some applications, and accounting for project costs. Some of the identified conditions from this report were also reported in prior Office of Audit reports. Specifically, these issues include:

- 2b, 2e-----
- EFDS Contingency plans were not updated and tested.
- EFDS Project costs were not accurate and complete.

Although management implemented corrective actions for these conditions, the actions did not resolve the past conditions.

Review of the Electronic Fraud Detection System

Specific concerns regarding the security of EFDS, delivery and effectiveness of some applications, and accounting for project costs follow.

Security of the System

Based on the sensitivity of the information processed, EFDS must meet Controlled Access Protection requirements, also known as C2 security requirements. EFDS obtained C2 security certification from the IRS certifying official on June 15, 1996. However, the issues discussed in this report illustrate that controls to prevent and detect unauthorized access to sensitive taxpayer data are not adequate within EFDS, and call into question whether EFDS should have received its unconditional security certification. We plan to separately review the certification process during Fiscal Year 1999.

Issues discussed in this report include the following:

- Access controls should be improved.
- The EFDS application audit trail -----
2b, 2e-----
- The EFDS application audit trail is 2b, 2e-----
2b, 2e---
- Security reviews at the service centers are not being performed.
- Security documentation is not current and, in some instances, does not reflect current system programming.
- Contingency plans need to be updated and tested.

We have the following recommendations related to the above issues.

The Project Office should work with EFDS developers to ensure there are adequate controls over user passwords, -----to ensure that audit trail records are maintained -----and to ensure audit trail records are accurate.

The Project Office should review the current C2 required documentation and update the information to reflect the current programming and operating procedures of EFDS. It should also ensure that EFDS contingency plans are updated and tested at least annually.

Information Systems (IS) should clearly define, in the Internal Revenue Manual or other policy statements, who is responsible for performing security reviews on systems such as EFDS, and ensure that these reviews are performed.

We were informed that EFDS will soon undergo a new security certification. In our opinion, taking into account the audit trail and documentation issues discussed in this report, it is questionable whether EFDS should have received its prior security certification. In the upcoming certification process, IS should ensure that the issues discussed in this report are corrected, and that all other controls necessary for a proper certification are in place and functioning.

Review of the Electronic Fraud Detection System

Delivery and Effectiveness of Some Applications

EFDS will meet all of its stated goals only after all requested applications are delivered and properly functioning. EFDS was not functioning as designed when sorting cases to ensure returns with the highest potential for fraud are reviewed first. Also, some EFDS applications are not being delivered timely by contract developers.

We recommend that the EFDS Project Office ensure program changes are made to EFDS which would allow returns with the highest fraud potential to be worked first. Also, the Project Office and CID should reach formal agreement on the requirements for EFDS. When the functional requirements are delivered, the Project Office should give timely, complete, and detailed feedback regarding changes necessary to the functional requirements.

Accounting for Project Costs

Improvements are needed to accurately account for EFDS costs. The Project Manager has not ensured that cost figures maintained by the Project Office were complete or accurate. We identified accounting discrepancies in Project Office records that resulted in total costs being understated by \$22.3 million. IRS officials need complete, accurate, and reliable accounting data to make informed decisions regarding EFDS costs and benefits.

Using the information we developed as a starting point, we recommend that the Project Office make a thorough review of EFDS cost records to ensure that no other misstatements or omissions have occurred. Also, the Project Office should maintain a schedule to track both non-Project Office and Project Office costs, and should reconcile its cost data to source documentation and to the Automated Financial System (AFS) on a regular basis.

Management's Response: IS management agreed with the findings and has developed the following corrective actions to address the issues:

- The EFDS Project Office has taken steps to strengthen password controls and will work with the Assistant Commissioner for Program Management and Architecture to strengthen access controls and to improve the system's audit trail capabilities.
- All C2 security documents and contingency plans will be updated according to guidelines. The EFDS Project Office will ensure all controls necessary for security certification are in place.
- The IRS' Office of Security Standards and Evaluation agreed to perform management reviews to ensure that security reviews of EFDS and other sensitive systems are performed.

Review of the Electronic Fraud Detection System

- EFDS programming was changed to allow priority returns with the highest fraud potential to be worked first in processing year 1999. In addition, the EFDS Project Office is in the process of implementing a Configuration Control Board, and Requirements Traceability within the project which will require all partners to agree to the requirements of the system before they are forwarded for approval.
- The EFDS Project Office will use cost information identified during this audit as a beginning and will use IRS mandated systems to continue to track and reconcile costs.

We concur with the corrective actions outlined in their response. Their response is incorporated into the body of the report where appropriate. The complete text of management's response is presented as Appendix V.

Review of the Electronic Fraud Detection System

Objective and Scope

The overall objective of our review was to determine if EFDS was functioning effectively and if the system was meeting proper control standards.

This report presents the results of our review of the effectiveness of the Electronic Fraud Detection System (EFDS). The audit was performed at the Ogden and Cincinnati Service Centers and the EFDS Project Office in Washington, DC in accordance with *Government Auditing Standards*. The review was performed from February through September 1998. The overall objective of our review was to determine if EFDS was functioning effectively and if the system was meeting proper control standards. To accomplish this objective, we evaluated whether:

- EFDS had met its program goals and objectives.
- The Project Office had established adequate security and operating controls to safeguard taxpayer data.
- The Project Office maintained reliable project cost data.

Appendix I contains the detailed objectives, scope and methodology for this review. A listing of major contributors to the report is shown in Appendix II.

Background

With the advent of electronic filing in 1986, the number of tax returns claiming fraudulent refunds has dramatically increased. This caused concern to both IRS and external oversight bodies. As a result of these concerns, EFDS was developed by the IRS Research Division, the Los Alamos National Laboratory (LANL), and the Criminal Investigation and Electronic Filing Branches at the Cincinnati Service Center. Shortly after its initial development, EFDS was assigned a project office to oversee future development and improvement of the system. At its inception, EFDS had the following four basic goals:

Review of the Electronic Fraud Detection System

- Automate the labor-intensive manual screening process of the Questionable Refund Program.
- Improve scoring techniques to reduce excessive volumes and to ensure that returns with the highest potential for fraud were reviewed.
- Increase data sources to improve detection of fraud.
- Enhance scheme development for referral to the districts for criminal prosecution.

During 1994, EFDS was prototyped at the Cincinnati Service Center. In 1995, a limited version was implemented in the other Electronic Filing (ELF) Service Centers. In 1996, additional workload management features were included and the system was further rolled out to the non-ELF Service Centers. For 1997 and 1998, the Project Office concentrated on stabilizing and strengthening the current system applications before adding to the system. It has also been preparing the system to become Year 2000 compliant. For the years ahead, the EFDS Project Office plans for the addition of a Scheme Tracking and Referral Subsystem and further integration of fraud detection tools developed by LANL.

Results

Overall, EFDS has been effective in meeting most of its program goals and the needs of its users.

Overall, EFDS has met most of its program goals and the needs of its users. With this system, IRS has automated the labor intensive manual screening process of the Questionable Refund Program, increased the data sources available for fraud detection, and has enhanced scheme development through its ability to more concisely examine return information for fraud potential.

Prior to EFDS, Criminal Investigation Division (CID) Tax Examiners scanned large volumes of paper Wage Information Fact Sheets that contained current year return information. They were limited to current year information unless they individually researched prior year information on the Integrated Data Retrieval System. With EFDS, these tax examiners now scan

Review of the Electronic Fraud Detection System

potentially fraudulent returns on a computer screen that displays all current year ELF return information, as well as summary information from prior year returns and employers. Thus, examiners are better able to determine fraud potential because more information is available on one screen. In addition, EFDS provides the ability for users to perform their own research through query capabilities. The query capabilities help users to identify schemes by identifying additional returns meeting specific characteristics.

During the initial phases of EFDS, LANL was a major participant in implementing the system. However, the primary purpose of LANL was to develop new methods of finding fraud. After evaluating this primary purpose, CID found the results to be mixed. The IRS has spent over \$9.4 million for LANL's assistance in developing EFDS. Tools for improved fraud detection have been scheduled for delivery since 1996; however, as of September 1998, tools capable of being implemented had not been delivered. According to CID managers, their main reason for recommending that the LANL contract not be renewed was due to LANL's inability to deliver products that ultimately aided in the detection of fraudulent returns. It is unclear at this time what additional benefits EFDS will receive from LANL's fraud detection efforts. Based on these facts, we agree with the decision made by both the CID and the EFDS Project Office to discontinue further development by LANL.

We agree with the decision made to discontinue further development by LANL.

While EFDS has experienced many successes, we identified issues of concern regarding:

- Security of the system.
- Delivery and effectiveness of some applications.
- Accounting for project costs.

These concerns are discussed below.

Review of the Electronic Fraud Detection System

EFDS must meet Controlled Access Protection requirements, also known as C2 security requirements.

Security of the System

Based on the sensitivity of the information processed, EFDS must meet Controlled Access Protection requirements, also known as C2 security requirements. C2 requirements are identified in the Department of Defense Trusted Computer System Evaluation Criteria, commonly referred to as the Orange Book. The requirements include accountability of users through login and password procedures, discretionary access control mechanisms, audit of security-relevant events, and object reuse. EFDS obtained C2 security certification from the certifying official on June 15, 1996. However, based on the results of our security tests discussed below, we question whether EFDS should have been given unconditional certification. A more detailed discussion of C2 security requirements is contained in Appendix VI.

As part of our review of the effectiveness of EFDS, we performed a number of tests to evaluate the adequacy of EFDS security controls. These tests were performed at the Ogden and Cincinnati Service Centers. Some testing was also performed at each of the other EFDS host sites (Andover, Austin and Memphis Service Centers).

Access Controls Should Be Improved

The EFDS system currently resides on a 2b, operating system. The EFDS application contains software programs which interface with 2b, 2e databases. We found areas of concern with the security of both the 2b, 2operating system and the EFDS application. The EFDS Project Office made the decision to replace the 2b, 2operating system with 2b, 2e----- 2b,prior to processing tax returns in 1999. They informed us that this change will address our concerns regarding the 2b, 2operating system; however, the change will have no effect on the EFDS application.

To access EFDS, two sets of passwords are required. 2 2b, 2e-----

2b, 2e-----

2b, 2e-----

**Review of the
Electronic Fraud Detection System**

2b, 2e----- We were successful in 16 of 16 attempts at the Ogden Service Center and 12 of 25 attempts at the Cincinnati Service Center. Six of the 12 Cincinnati Service Center passwords were assigned to the users on the same day we performed our test. Our successful accesses included 2b, 2b, 2e-----
2b, 2e----- If a user accessed the EFDS application through one of these passwords, the user would have database administrator capabilities, which would allow this user to browse taxpayer data undetected, allow other unauthorized users access to sensitive data, and determine what returns are reviewed by tax examiners in the CID.

- 2b, 2e-----

2b, 2e-----

**Review of the
Electronic Fraud Detection System**

2b, 2e-----

We reviewed the EFDS application audit trail reports and interviewed system administrators at the Ogden and Cincinnati Service Centers to determine if audit trail records 2b, 2e-----

2b, 2e----- (At the time of our review, there were no audit trails running for the 2b, 2e operating system. The Project Office was in the process of implementing this audit trail.)

2b, 2e-----

2b, 2e----- An audit trail exception report would assist in doing this.

We presented the information regarding access controls to management in an Audit Memorandum dated June 4, 1998. In that memorandum, we recommended that the Director of Investigations, Office of Refund Fraud, take the following actions:

Until systemic changes are made, reemphasize security procedures found in the "EFDS Account and User Policy" created on September 5, 1997. Criminal Investigation Branch Chiefs should document and attest that EFDS security policies are being followed. This issue should also be addressed in Criminal Investigation Branch operational reviews.

The Director of Investigations, Office of Refund Fraud, concurred with our recommendation and took

Review of the Electronic Fraud Detection System

appropriate corrective action. A copy of his response is included as Appendix IV of this report.

We also made the following recommendations to Information Systems (IS).

Recommendations

The EFDS Project Office should work with EFDS developers to ensure that the following programming changes are made:

1. 2b, 2e-----

2. 2b, 2e-----

3. 2b, 2e-----

4. 2b, 2e-----

Management's Response:

To address these issues, IS management provided the following information:

- 2b, 2e-----

- 2b, 2e-----

[illegible]

- [illegible]

=====
 =====
 =====

$$\begin{array}{l}
 2b, 2e \text{-----} \\
 \text{-----} \\
 2b, 2e \text{-----} \\
 2b, 2e \text{-----} \\
 2b, 2e \text{-----} \\
 \text{-----} \\
 2b, 2e \text{-----}
 \end{array}$$

2b, 2e-----

- _____
- _____
- _____
- _____

2b, 2e-----
 2b, 2e-----

Review of the Electronic Fraud Detection System

system administrators, we determined that 2b, 2e-
2b, 2e-----
2b, 2e----- Although secondary accesses
are a small percentage of the overall use of EFDS,
the IRS 2b, 2e-----
2b, 2e-----

- *In some instances, actions listed on the EFDS application audit trail are incorrect.*

The EFDS application audit trail contains some information that is incorrect.

When a taxpayer's account has previously been accessed by a user, subsequent accesses to that account cause the EFDS application audit trail to record both the subsequent access and an additional incorrect access to the audit trail record. For example, if user #1 accessed an account on February 1, 1998, this user would generally be recorded on the audit trail as accessing the account on February 1, 1998. If another user, user #2, accessed the same account on March 1, 1998, the audit trail would generally show user #2 as accessing the account on March 1, 1998. However, at the time the second entry is recorded, a third incorrect entry is also recorded showing user #1 as also accessing the account on March 1, 1998. We accessed 30 taxpayer records that had been previously accessed by other tax examiners. In all 30 cases, the audit trail incorrectly added the original tax examiners to the audit trail even though the original tax examiners did not access the accounts again.

The audit trail incorrectly added the original tax examiners to the audit trail even though the original tax examiners did not access the accounts again.

In addition to the above condition, it was brought to our attention that some entries to the Ogden Service Center's EFDS application audit trail showed users accessing accounts late on a Sunday night when they were not at work. We reviewed the tax examiners' audit logs and verified that they were not on the system at the time. We verified that this was also happening at the Cincinnati and Memphis Service Centers. We had a tax examiner at the Ogden Service Center do a D2K query on accesses to the Ogden Service Center host site accounts (contains

Review of the Electronic Fraud Detection System

Ogden and Fresno Service Center data) on Sunday, March 29, 1998, and Sunday, April 5, 1998. The D2K query showed 1,764 records listed on the application audit trail for March 29, 1998, and 1,651 records for April 5, 1998. We were informed by the Ogden Service Center's EFDS system administrator that this condition had something to do with a specific program that is run each Sunday night in Ogden. We contacted the system administrator in Memphis and found that the same program run there also correlated with accesses listed on the Memphis Service Center's EFDS application audit trail report. These accesses were also recorded during regular off-duty hours (such as 2 a.m. Friday morning).

Both conditions cause the EFDS application audit trail to be unreliable because individual accountability has been tainted.

Both of these conditions cause the EFDS application audit trail to be unreliable because individual accountability has been tainted. These conditions also cause the audit trail to be inefficient due to the invalid entries that take up system space and memory.

Recommendations

The EFDS Project Office should work with EFDS developers to ensure that the following programming changes are made:

5. 2b, 2e-----

6. 2b, 2e-----

7. Determine why the EFDS application audit trail is recording inaccurate or unnecessary entries. Reprogram the audit report segments of the system to accurately reflect user actions on the system.

Review of the Electronic Fraud Detection System

Management's Response:

In their response, IS managers stated:

- Conversion to 2b, 2e-----and the accelerated time frame for Year 2000 deliverables preclude their taking immediate corrective action with current funding. However, the EFDS Project Office has requested the Assistant Commissioner for Program Management and Architecture to review, evaluate and assist in formulating a plan for the interface between EFDS and the Audit Trail Lead Analysis System (ATLAS) that will address the audit trail 2b, 2e-----
2b, 2e----- The EFDS Project Office will use Internal Revenue Manual (IRM) section 2.1.10 as the basis for the overall design of the audit trail.
2b, 2e-----
2b, 2e----- The EFDS Project Office has modified its requirements to include this task.
- All programming issues relating to the recording of inaccurate or unnecessary entries have been corrected.

The EFDS Application Audit Trail Is 2b, 2e----- 2b, 2e-----

*Audit trail reports are
2b, 2e-----
2b, 2e-----
2b, 2e---*

As stated earlier, the EFDS application can generate four different audit trail reports. These reports consist of the Program Audit Trail Report, Return Audit Trail Report, W-2 Audit Trail Report, and DLN Summary Audit Trail Report. We believe these reports are 2b, 2e-----
2b, 2e-----

Review of the Electronic Fraud Detection System

- The EFDS application audit trail reports are 2b,
2b, 2e-----

- The audit trail reports use the DLN of the return accessed as the account identifier.
- The records contained in the reports are cumulative from the beginning of each processing year and cannot be segmented by 2b, 2e-----

A DLN is unique to a specific tax return but is difficult to associate with a specific taxpayer.

The reports most likely to be used to review for browsing would be the DLN Summary or the Return Audit Reports. However, both of these reports use the DLN of the return accessed as the account identifier. A DLN is unique to a specific tax return but is difficult to associate with a specific taxpayer. DLNs change as adjustments are made to returns, and taxpayers have different DLNs for each return they file. In contrast, taxpayers have only one SSN which should never change. 2b, 2e-----

2b, 2e-----

2b, 2e-----

2b, 2e-----

2b, 2e-----

2b, 2e-----

2b, 2e----- In addition, if fields such as Name Control and Zip Code were also added, analyses could be performed to identify instances where employees accessed accounts containing a last name similar to their own and accounts with addresses close to their own address. Any of these instances could indicate that an employee may be browsing a relative's or acquaintance's account.

The records contained in the Program Audit Trail and Return Audit Trail Reports cannot be segmented by 2b, 2e----- For example, if a manager at the Ogden Service Center reviewed the Return Audit Report and selected the "All TE" button, the report would contain data for both the Ogden host site and the Fresno Service Center remote site. If this report is generated toward the

Review of the Electronic Fraud Detection System

end of the tax season, the report can be very lengthy and cumbersome. In fact, in March when we tried to generate the Return Audit Report for all tax examiners at the Ogden Service Center, the report would not generate. The system administrator at the Ogden Service Center informed us that the report would not generate because the size of the audit report exceeded the available space allocated to generate the report. The same thing happened when we tried to generate the Return Audit Report at the Cincinnati Service Center.

- The EFDS application 2b, 2e-----
2b, 2e-

The EFDS application

2b, 2e-----

2b, 2e-----

2b, 2e-----

The EFDS application 2b, 2e-----

2b, 2e-----

2b, 2e-----

2b, 2e-----

2b, 2e----- To test the application, three

auditors at the Ogden Service Center accessed their

own accounts. 2b, 2e-----

2b, 2e-----

Review of the Electronic Fraud Detection System

A memorandum of understanding regarding controlling unauthorized accesses to taxpayer information was signed by IRS Executives in August and September 1997. The memorandum of understanding calls for the Chief Information Officer (CIO) to: ensure that all IRS information systems contain suitable and operational audit trails; and assess the systems that process and contain taxpayer data to determine which systems have audit trails and how those audit trails work. The assessment should contain recommendations to improve the use of specific audit trails and be provided to IRS executives. However, the Centralized Case Development Center (CCDC) had not received an assessment for EFDS.

Recommendations

8. The EFDS Project Office should work with EFDS developers to ensure that the following programming changes are made:
 - The EFDS application audit reports -----
2b, 2e-----

 - Adequate file space should also be allocated to ensure available space to generate the reports.
9. The CIO should complete the assessment discussed in the September 1997 memorandum of understanding, taking into consideration the audit trail issues referred to in this memorandum to improve the usefulness of the EFDS application audit trail. Consideration should be given to audit trail elements that will 2b, 2e-----
2b, 2e-----

The CCDC should assist the CIO's staff in developing specific audit trail requirements necessary for use in a Post Audit Analysis System, such as recording of significant events, capturing ample information, and accessing the event information.

Review of the Electronic Fraud Detection System

10. Because of the sensitivity of the data maintained on EFDS, and the number of people who have access to the system (with more planned in the future), the audit trail problems referred to in the report should be included by the IRS as a Federal Manager's Financial Integrity Act (FMFIA) material weakness.

Management's Response:

IS management provided the following:

- The plan formulated by the EFDS Project Office and the Assistant Commissioner for Program Management and Architecture will address:
 - Implementing the recommended design of an audit trail application that 2b, 2e-----

 - Designing the audit trail 2b, 2e-----
2b, 2e-----
 - Ensuring the audit trail will 2b, 2e-----
2b, 2e-----

The EFDS Project Office will use IRM section 2.1.10 as the basis for the overall design of the audit trail.

- For processing year 1999, the system has been sized to accommodate report generation.
- The IRS' Security Infrastructure Implementation Plan (120-Day Report), dated November 7, 1997, responded to the memorandum of understanding. It identified system capabilities, deficiencies, and enhancements planned. For EFDS, it noted that automated analysis tools are not available but that this would be enhanced with the deployment of future architecture. In this regard, it is also noted that the Interim Regional Infrastructure System (IRIS) is intended to audit all events and will forward this information to an authoritative data repository and analysis system. IRIS is scheduled to be deployed as part of the Phase 1, Sub-release 1.3

Review of the Electronic Fraud Detection System

of the IRS Modernization Blueprint Sequencing Plan.

- A conference call was held on August 13, 1998, between the EFDS Project Office, the EFDS programming contractor and the CCDC to work out EFDS audit trail issues. EFDS is prepared to furnish whatever information is required after being given the audit program record requirements and examining methods for file transfer program retrieval by the Center. A subsequent meeting was held on October 22, 1998, by the EFDS Project Office to further develop the CCDC audit trail data requirements with the assistance of the Assistant Commissioner for Program Management and Architecture.
- Audit trail weaknesses are currently included in the FMFIA material weakness for Service Center security, which is being addressed in the security plans currently being overseen by the Office of Security Standards and Evaluation.

EFDS Security Reviews at the Service Centers Are Not Being Performed

Of the six service center sites contacted, only one had performed a security review of EFDS.

The IRM states that the IS Security function at each service center is responsible for performing annual evaluative reviews along with compliance reviews of each information system. This manual also states that the Office of Security Standards and Evaluation is responsible for ensuring that these reviews are performed. We interviewed personnel from the IS Security functions located at six service centers to determine if their offices had ever performed any security reviews pertaining to EFDS. Of the six sites contacted, only one had performed a security review of EFDS. Reasons given for not performing the reviews included lack of resources and questions as to who was responsible for performing the EFDS reviews.

Review of the Electronic Fraud Detection System

The IRS Information Systems Security Program is outlined in IRM 2 Section 10. The purpose of the Security Program is to:

- Assure adequate security is provided for all data collected, processed, transmitted, stored, or disseminated on information systems and networks.
- Ensure the confidentiality, integrity, and availability of information.
- Provide for the protection of individual, proprietary, financial, tax, mission-critical, or otherwise sensitive information.
- Ensure the ability to maintain processing during and following an emergency.
- Ensure management and employee accountability for computing resources including data and information entrusted to them is accomplishing IRS objectives.

If proper security reviews are not performed on the IRS information systems, the IRS will have no way of determining if it is meeting its Information Systems Security Program objectives.

If proper security reviews are not performed on the IRS information systems, the IRS will have no way of determining if it is meeting its Information Systems Security Program objectives.

Recommendation

11. IS should clearly define in IRS' IRMs or other policy statements who is responsible for performing security reviews on systems such as EFDS, and ensure that these reviews are performed.

Management's Response:

IS management pointed out that IRM 2.1.10, Information Systems Security, Section 10.4, Security Guidelines Overview, provides information systems security guidelines, including individual duties and responsibilities for security reviews. The IS Security and Certification Program Office has the responsibility for ensuring that this IRM is updated and current.

The IRS' Office of Security Standards and Evaluation agreed to perform management reviews to ensure that

Review of the Electronic Fraud Detection System

security reviews of EFDS and other sensitive systems are performed. These reviews are now ongoing.

Security Documentation Is Not Current and, in Some Instances, Does Not Reflect Current System Programming

EFDS is required to meet C2 security criteria.

As previously stated, EFDS is required to meet C2 security criteria. Part of the C2 criteria requires the following documentation:

- Security Features User's Guide (formerly Users Guide) – A single summary, chapter, or manual in the user documentation shall describe the security features provided by the information system, guidelines on how to use them, and how they interact with one another.
- Trusted Facility Manual (formerly System Guide) – A manual addressed to the system administrator, operator, and Information Systems Security Staff which presents cautions about functions and privileges that must be controlled when running a security facility. The manual shall also include the procedures for examining and maintaining the relevant information for each high-risk access.
- Security Test and Evaluation Report – A document shall be provided which describes the test plan and results of the security features functional testing.
- Design Documentation – Documentation shall describe the philosophy of security protection and an explanation of how this philosophy is implemented and required for each information system.

C2 criteria requires the following documentation: Security Features User's Guide, Trusted Facility Manual, Security Test & Evaluation Report, and Design Documentation.

In reviewing the EFDS C2 documentation, we identified statements referring to security features which are not in place on EFDS, such as 2b, 2e-----
2b, 2e-----
2b, 2e----- In addition, the documentation lacked references to necessary security features, such as application audit trail procedures. Throughout the documents, there are also references to the 2b,

Review of the Electronic Fraud Detection System

operating system. Because EFDS will be converting over to the 2b, 2e-----operating system, references to the 2b, system in this documentation will also become outdated.

The EFDS Security Features User's Guide contains the following statement: "...through understanding implemented security mechanisms, users are able to consistently and effectively protect IRS-maintained information." However, if the information found in the C2 documentation is not accurate or does not reflect current system programming, users could rely on controls which are not functioning and compromise the security of the system. For example, if a CID manager relied on the documentation found in the EFDS Users Guide, which states that EFDS user passwords expire after 16 weeks have elapsed, it could cause the manager to rely more on the password aging control and less on manual procedures which instruct the manager to ensure that passwords are changed periodically.

We were informed that EFDS will soon undergo a new security certification. In our opinion, taking into account the audit trail and documentation issues discussed in this report, it is questionable whether EFDS should have received its prior security certification.

Recommendations

12. The EFDS Project Office should review the current C2 required documentation and update the information to reflect the current programming and operating procedures of EFDS.
13. In the upcoming certification process, IS should ensure that the issues discussed in this report are corrected, and that all other controls necessary for a proper certification are in place and functioning.

Review of the Electronic Fraud Detection System

Management's Response:

IS management agreed to take the following corrective action:

- C2 re-certification began in May 1998. All C2 documents will be updated according to guidelines. Management has secured a contractor to assist in performing this task.
- The EFDS Project Office has begun the new security certification process. A Statement of Work was prepared for a contractor to perform the security certification. Currently, the contract costs are being negotiated and work is expected to begin soon. The Project Office will ensure issues are corrected and all other controls for certification are in place. Management provided a copy of this audit report to the IS Certification Program Section (IS:O:O:S:C) to ensure all issues are corrected and that all other controls necessary for certification are in place and functioning.

Contingency Plans Need to be Updated and Tested

It is the responsibility of agencies, through contingency planning, to "...establish and periodically test the capability to perform the agency function supported by information systems in the event of failure of its automated support."

Office of Management and Budget Circular No A-130, *Management of Federal Information Resources*, dated February 8, 1996, establishes the policy to manage federal information resources. The Circular states that it is the responsibility of agencies, through contingency planning, to "...establish and periodically test the capability to perform the agency function supported by information systems in the event of failure of its automated support. Agency plans should assure that there is an ability to recover and provide service sufficient to meet the minimal needs of users of the system." The IRM states that these plans should be tested at a frequency commensurate with the risk and importance of loss or harm that could result from disruption of information system support but not less than once a year.

Review of the Electronic Fraud Detection System

We reviewed the EFDS contingency plan dated December 1995. One of the main controls presented in the plan relies on the 2b, 2 located at the Cincinnati Service Center, to be operational and available to serve as the EFDS backup site. However, the 2b, has been unsuccessful as a backup system and has now been converted to a Production Development System for future testing and development. EFDS now relies on tape backup at each site for system recovery. Although the 2b, is no longer functioning as a system backup, the EFDS contingency plan has not been updated to reflect this fact. In addition, none of the three EFDS site system administrators we interviewed had ever seen an official EFDS contingency plan or were aware of any specific tests done to test the plan.

By not having adequately updated and tested contingency plans, the IRS does not have assurances that procedures will be in place for EFDS users to effectively evaluate tax returns in the event of minor system failures or a full-scale shutdown of the EFDS.

By not having adequately updated and tested contingency plans, the IRS does not have assurances that procedures will be in place for EFDS users to effectively evaluate tax returns in the event of minor system failures or a full-scale shutdown of the EFDS. Thus, fraudulent refunds may not be timely identified and stopped. In addition, the system's ability to restore data after a shutdown remains uncertain without proper contingency testing.

Recommendation

14. The EFDS Project Office should ensure that EFDS contingency plans are updated and tested at least annually. In addition, the plans should be made available to all concerned parties (system administrators, CID system users, etc.).

Management's Response:

IS management stated that the documents were not updated due to numerous program and system enhancements over the past few years. However, contingency plans were known and shared with the systems and database administrators (SA/DBA) and the end user. The final contingency is the use of the paper system. The contingency plan will be updated to reflect the system in place for processing year 1999. Each site

Review of the Electronic Fraud Detection System

is required to backup the EFDS data and contingency testing is scheduled locally. Each site SA/DBA has also been provided training at the annual SA/DBA training session to allow them to perform backup and recovery processes for a number of items which could occur in a normal production environment.

Delivery and Effectiveness of Some Applications

EFDS Does Not Sort Cases to Ensure Returns With the Highest Potential for Fraud Are Reviewed First

The Prescan Screen is the main screen within EFDS. Each day, this screen shows returns that have been selected for review. This screen provides the tax examiner with a variety of information to assist in the determination of potential fraud.

The Questionable Refund Program training handbook states that Prescan workload is sorted with the intent of “floating” returns with the highest fraud potential to the top of the “pile.” This would ensure that the returns with the highest fraud potential would be worked first. According to the handbook and input from the Project Office, the work is sorted by 1) District; 2) Part Number; 3) Refund Stop Date; and 4) Questionable Refund Score. We reviewed 50 returns (30 from Ogden Service Center and 20 from Cincinnati Service Center) and found that the returns with the highest Questionable Refund Scores were not floated to the top of the inventory to be worked first. The returns we compared all had the same District, Part Number, and Refund Stop Date. We found from our test that lower scored returns are being given out when there are many higher Questionable Refund scored returns in inventory ready to be worked.

Returns with the highest fraud potential are not being worked first.

If the highest Questionable Refund scored returns are not worked first, the IRS risks that some of these returns might not get worked. Currently, the program sorts the

Review of the Electronic Fraud Detection System

returns with the highest fraud potential once they are downloaded into groups of 25. As long as all groups are worked timely, there is no real effect from not working the returns with the highest fraud potential first. However, if the system went down or if staffing resources did not allow working all cases within each stop date, refunds with higher fraud potential could be issued before a tax examiner reviewed them.

Recommendation

15. The EFDS Project Office should ensure that program changes are made to EFDS which would allow returns with the highest fraud potential to be worked first.

Management's Response:

IS management stated that the changed application which allows priority returns with the highest fraud potential to be worked first was corrected for processing year 1999.

Some EFDS Applications Are Not Being Delivered Timely by Contract Developers

*CID does not have the
functionality they had planned
from EFDS.*

Although EFDS has met many of CID's needs as stated earlier, there are a number of EFDS applications which have not been implemented timely. Three of these applications are as follows:

- **Contact Employer:** Contact Employer is being designed within EFDS as a workload management system for Forms W-2 or other income documents requiring verification from employers.
- **STARS:** The Scheme Tracking and Referral System (STARS) is being designed as a subsystem of EFDS that tracks the status and results of Questionable Refund Program schemes for both ELF and paper returns. It will provide a variety of management and other statistical reports for use by IRS Executives,

Review of the Electronic Fraud Detection System

Treasury, and the Congress concerning fraud detection efforts.

- LANL Tools: LANL designed a new workload management system known as Case. When functional, Case will allow tax examiners to work “groups” of similar returns rather than one return at a time. Returns will be generated in Case through a variety of Automatic Case Generation Mechanisms that create cases based upon certain return criteria or through other “interactive” tools such as Link and Profiler. Link and Profiler are tools that will allow users to identify trends or similarities among returns and then assign these returns to be worked within the Case workload management system.

According to EFDS Business Cases, certain EFDS features were to be operational for 1996 and 1997. As yet, these features have not been implemented or are not currently functioning.

According to the 1995 EFDS Business Case, certain LANL tools (Link & Profiler) and Workload Management features (Contact Employer) were to be operational for 1996. Additionally, the 1996 EFDS Business Case called for STARS to be operational by 1997. As yet, these applications have not been implemented or are not currently functioning. STARS was scheduled to be implemented in January 1999 and the LANL tools & Contact Employer are scheduled to be implemented in January 2000.

There were various explanations given for the missed delivery dates. We were unable to determine the exact cause for each application. We were given information about a number of factors that could have affected the delivery of these applications.

- LANL’s original purpose was to develop new techniques for identifying fraudulent returns. However, it appears that LANL has been more research-oriented than production-oriented. They have been unsuccessful in converting their research ideas to final usable products. In addition, adequate oversight may not have been provided in monitoring LANL’s efforts. A CID memorandum dated May 22, 1998, stated the following: “Office of Refund Fraud and the Project Office by fall of 1996 lacked knowledge of the details of LANL work.

Review of the Electronic Fraud Detection System

Criminal Investigation Division management in the Office of Refund Fraud asserted itself to correct this.”

- EFDS was initially developed using an accelerated Systems Development Life Cycle approach. This approach caused some applications to be rolled out before they were completely functional and useful. As a result, the Project Office had to reprogram and rework some of the applications. The Project Office is no longer using the accelerated Systems Development Life Cycle and has committed to fully develop these applications before implementation.
- STARS may have been delayed because complete requirements had not been provided to the contractor. There is a disagreement between the EFDS Project Manager and the CID on this issue. CID management believed they had delivered complete requirements, however the Project Manager disagreed.

Recommendation

16. The Project Office and the CID should reach formal agreement on the requirements for EFDS. When the requirements are delivered, the Project Office should give timely, complete, and detailed feedback regarding necessary changes.

Management's Response:

IS management stated that System Development Life Cycle meetings, along with the appropriate walk-throughs, have been ongoing between EFDS Partners since August 1997. The EFDS Project Office is in the process of implementing Configuration Control Board (CCB) and Requirements Traceability (RT) within the Project. This requires all partners to agree to the requirements before they are forwarded for approval. The processes for RT need to be defined and implemented to assist the CCB in making informed decisions on requirements and changes within the system.

Accounting for Project Costs

Improvements Are Needed to Accurately Account for EFDS Costs

The Project Office has made some efforts to maintain appropriate cost records relating to EFDS. However, the Project Manager has not ensured that cost figures maintained by the Project Office were complete or accurate. We identified accounting discrepancies in Project Office records, which resulted in total costs being understated by \$22.3 million. This \$22.3 million included \$11.9 million in expenditures incurred by the IRS Research Division, and \$10.4 million in errors and omissions.

The EFDS cost data maintained by the Project Office is not accurate or complete and has resulted in understated cost data being used in official reports.

- *Expenditures incurred by the IRS Research Division were not included.*

In their response to a previous Office of Audit report, *Review of the Electronic Fraud Detection System Rollout* (Reference No. 061714), the Project Office agreed to identify and include costs incurred outside the Project Office in the total cost of the EFDS Project. In an effort to accomplish this, they identified and included \$3.4 million in hardware and software expenditures purchased before the Project Office was established.

However, in our review of Research Division documentation in the possession of the Project Office, we identified an additional \$11.9 million in costs that were not previously included in the total cost of the EFDS project. Included in this amount are contracts with LANL in Fiscal Years 1993 through 1996 totaling \$4.4 million; a contract with the Electronic Data Systems Corporation in Fiscal Year 1994 for \$2.5 million; and hardware, software, and maintenance purchases in Fiscal Years 1993 and 1994 totaling \$5 million.

Review of the Electronic Fraud Detection System

- Project Office cost data contained posting errors, math errors and omissions, which understated costs.

To ensure that expenditures do not exceed allocations, the Project Office tracks the annual allocations and expenditures for each of the EFDS Project Cost Accounting Subsystem (PCAS) codes they are assigned each year. However, the Project Office does not reconcile its cost data to supporting documentation or to the AFS (of which the PCAS is a subsystem) to ensure its accuracy. Our comparison of Fiscal Year (FY) 1997 Project Office costs to supporting documentation identified posting and math errors that overstated expenditures by over \$300,000. In addition, the Project Office could not provide detailed support for FY 1995 and FY 1996.

IRS managers need complete, accurate, and reliable data to make informed decisions regarding EFDS costs and benefits so that future functionality can be effectively and efficiently rolled out.

The Project Office does not maintain a master list of all EFDS PCAS codes to ensure that costs from each are included in the total cost of the project. In our comparison of Project Office cost data to AFS, we identified two PCAS codes whose related costs had not been included in the total cost of the project. The omissions understated total costs by \$10.7 million.

As a result, IRS managers may not get complete, accurate, and reliable data to make informed decisions regarding EFDS costs and benefits. For example, the EFDS Business Case prepared by the Project Office in September 1996 stated that project costs through the end of FY 1996 were \$46.3 million. Our review placed the actual expenditures in excess of \$56.4 million.

Recommendations

17. Using the information we developed as a starting point, the Project Office should make a thorough review of EFDS cost records to ensure that no other misstatements or omissions have occurred. The Project Office should maintain a schedule of non-Project Office costs and Project Office costs. The non-Project Office costs should include those costs identified in this review plus any other identifiable

Review of the Electronic Fraud Detection System

costs. The Project Office should maintain supporting documentation for each of these amounts. The Project Office costs should include costs for each EFDS PCAS code since FY 1995 when the Project Office was established. Each PCAS code amount should be supported by an AFS report containing the most current actual data. The sum of these two amounts is the total EFDS Project cost. This is the amount that the Project Office should use when preparing reports for or providing cost data to users outside of the Project Office.

18. The Project Office should reconcile its cost data to source documentation and to AFS on a regular basis. The amount recorded should be changed if the purchase order or an expenditure amount differs from the requisition amount. Reconciled Project Office cost data should be archived at the end of each fiscal year for future reference.

Management's Response:

IS management responded with the following:

- For FY 1994, (pre-Project Office) hardware and software was acquired through multiple sources. Therefore, historical documents were not centrally maintained. The Project Office requested and received all known historical documents in an effort to preserve this information. For FY 1995 and FY 1996, the financial process had been very volatile. Continuing Resolutions, No-Year funds, purchasing through the "exception" rule, all attributed to the inability to reconcile all monies to the *then* established PCAS codes. Management stated they will begin with the historical information already sorted via this investigation and use IRS mandated systems to continue to track costs.
- EFDS has made an effort to maintain accurate and appropriate cost records. Discrepancy reports were submitted to the AFS organization; however, fiscal year closure prohibited its update. The Project Office currently reconciles costs monthly between AFS and our source documentation. Reconciled

Review of the Electronic Fraud Detection System

Project Office cost data is archived at the end of each fiscal year.

Conclusion

With the development of the EFDS Project Office and through coordination with the CID, the IRS has achieved many successes relative to its development of EFDS. Overall, EFDS has been effective in meeting most of its program goals and the needs of its users. The Project Office is working toward added functionality to help increase the CID's ability to detect fraudulent returns.

While the system is a vast improvement over the manual procedures used prior to EFDS, there are still changes that can be made to further improve or manage the system.

While the system is a significant improvement over the manual procedures used prior to EFDS, there are still changes that can be made to further improve or manage the system. Security controls should be strengthened to help protect the taxpayer data contained within EFDS. The implementation of applications which have been in process for a number of years should be given priority for timely completion. Finally, the Project Office should implement controls to maintain accurate and complete cost data for the project.

Implementing recommendations made in this report will help ensure taxpayer privacy, protect revenue, and enhance the reliability of management information.

Detailed Objectives, Scope and Methodology

The overall objective for this review was to determine if the Electronic Fraud Detection System (EFDS) was functioning effectively and if the system was meeting proper control standards. To accomplish our objective, we performed the following sub-objectives and audit tests.

I. We determined if EFDS was meeting program goals and objectives.

- A. Determined if EFDS met its four basic goals to: automate the labor intensive manual screening process; improve scoring techniques to reduce volumes and ensure the highest potential fraudulent returns are reviewed first; increase data sources to improve detection; and enhance scheme development.
 - 1. Reviewed the EFDS Business Case and interviewed appropriate Criminal Investigation Division (CID) or EFDS Project Office personnel to learn the intent behind the goals and what was planned by management to achieve the goals.
 - 2. Interviewed CID personnel and reviewed EFDS user manuals or other documentation.
 - a) Identified the manual procedures, data sources available, and scheme development procedures used prior to EFDS.
 - b) Identified the EFDS procedures, the data sources used, the scoring techniques, and the scheme development procedures currently being used by EFDS.
 - 3. Interviewed CID managers and tax examiners to get their feedback concerning whether these goals had been met.
 - 4. Physically used some of the features of EFDS (prescan, query, etc.) and compared these features to the old manual screening procedures used prior to EFDS (paper Wage Information Fact Sheets).
 - 5. Reviewed a sample of 50 EFDS prescan cases (30 from the Ogden Service Center and 20 from the Cincinnati Service Center) from 10 different work “chunks” (5 cases from each “chunk”). Reviewed cases to determine if returns with the highest fraud potential were generated first.
 - 6. Compared the data sources available before EFDS to those now available through EFDS to determine if additional data sources were created with the establishment of EFDS.

Review of the Electronic Fraud Detection System

7. Reviewed CID reports, both before and after EFDS was developed to determine if:
 - a) EFDS was more efficient (work more cases per hour) than prior manual processing methods.
 - b) Improved scoring techniques have reduced the number of non-fraud returns reviewed.
 - c) Increased data sources improved fraud detection.
 - d) Scheme development procedures have improved.
- B. Determined if the system was meeting user needs.
 1. Interviewed tax examiners and managers at the Ogden and Cincinnati Service Centers to get input about system concerns and whether EFDS was meeting their needs. Specifically, determined if users were comfortable using the various features of the system and if they received adequate training for using these features.
 2. Reviewed available Integrated Network and Operations Management System (INOMS) reports of the National Office Command Center (NOCCs) and determined if identified problems were being resolved timely.
 - a) Contacted employees at INOMS Help Desk and requested a list of NOCCs issues closed during calendar year 1997 and any open NOCCs issues.
 - b) Reviewed a sample of 30 closed NOCCs issues to determine if they were closed timely and properly resolved.
 - c) Reviewed a sample of 20 open NOCCs issues to determine if any serious problems were not being timely addressed.
 3. Determined if quality measurements had been established for EFDS.
 - a) Interviewed Project Office personnel to determine if a quality measurement plan has been established.
 - b) Reviewed the measurements to determine if they seemed adequate and whether they showed if the system was meeting the goals of users.
 4. Determined if adequate system testing had been performed.
 - a) Interviewed Information Systems (IS) and Project Office personnel to determine if acceptance (hardware & software) and capacity (Central Processing Unit, memory, disk capacity) testing had been performed on the system.

Review of the Electronic Fraud Detection System

- b) Obtained a copy of the current Systems Acceptability Testing (SAT) plan and reviewed to ensure the SAT team evaluated whether there were adequate controls in place to ensure the cases were properly controlled and the data was accurate on the system.
- c) Determined if the SAT team sufficiently reviewed the reports from EFDS to ensure they were accurate as well as adequate for IRS management's needs.
- d) Determined if the SAT team reviewed the run controls to ensure that all cases were properly controlled.
- e) Reviewed the controls for Forms 5534 to determine if problems identified by SAT on the system were resolved timely and were properly controlled.
- f) Determined if the EFDS program and test data were ready to be reviewed when the SAT team was scheduled to begin.
- g) Reviewed the SAT schedule to determine if the test completion dates were reasonable.

II. We determined if EFDS data were safeguarded and being used appropriately.

- A. Evaluated the overall effectiveness of EFDS security and operating controls.
 - 1. Determined if controls (e.g., password assignment) were in place and functioning properly to ensure that only authorized personnel had access to the host site systems in the Ogden and Cincinnati Service Centers.
 - a) Interviewed IS personnel and review procedures at the Cincinnati and Ogden Service Centers to determine if controls were in place at the host sites.
 - b) Determined if passwords were used to access the system and requirements existed to change passwords on a frequent basis. Also determined if passwords were required to enter the system through external sources such as the D2K Browser, data base administrator terminals, and Los Alamos terminals.
 - c) Determined if the system had the ability to allow or deny access by specific users to specific information and/or applications.
 - d) Obtained a list of users and their user capabilities and reviewed for reasonableness (e.g., tax examiners do not have management capabilities, former employees are deleted from the system).

Review of the Electronic Fraud Detection System

- e) Determined if it was common for data to be transferred off sight and whether the data was protected by encryption or other authorized safeguards.
 - f) Determined what taxpayer information was available to contract vendors and if it was appropriate for them to have the information. Also determined if taxpayer information given to contract vendors was properly safeguarded.
 - g) Determined if security checks were properly performed on contract vendor personnel.
 - h) Determined if a security officer had been established and that the duties for this job were being performed.
 - i) Determined if the following security documents existed for EFDS:
 - 1) Security Features User's Guide - A document describing the system security features, how to use them, and how they interact.
 - 2) Trusted Facility Manual - A document stating the cautions to be observed in controlling functions and privileges. Also, procedures for maintaining and examining the audit trail records.
 - 3) Test Documentation - Procedures for testing security features, and the results of such tests.
 - 4) Design Documentation - A document describing the manufacturer's philosophy of protection and how this is built into the information system.
2. Determined if system contingency plans had been developed and whether proper backup and recovery procedures were in place in the event of a system failure.
- a) Interviewed host site administrators and Project Office personnel to determine if a contingency plan existed and what backup and recovery procedures were in place for the Ogden and Cincinnati Service Center host sites.
 - b) Reviewed the plan and recovery procedures to determine if controls were adequate.
 - c) Determined if the plan had been tested and the results of any tests.
3. Determined if EFDS was Year 2000 (Y2K) compliant or had plans to become Y2K compliant.

Review of the Electronic Fraud Detection System

- a) Interviewed the project manager and the Y2K coordinator regarding Y2K compliance of the system.
 - b) Reviewed documentation regarding system compliance.
 - c) Determined what plans the Project Office had to make the system Y2K compliant.
 - d) Reviewed the plans for timeliness and adequacy.
4. Evaluated the effectiveness of, and compliance with, new internal controls implemented by the Chief Information Officer organization, including the direction and oversight provided by the following offices:
- a) Government Program Management Office.
 - b) Systems Standards and Evaluation Office.
 - c) Performance Management Office.
- B. Determined if controls were in place to identify the inappropriate use of EFDS taxpayer data.
1. Determined what taxpayer information was available on EFDS and if the possibility existed that unauthorized accesses to the information could occur.
- a) Determined what taxpayer information was available on EFDS and the System Recovery Server.
 - b) Determined the number of users who had access to EFDS.
 - c) Attempted to determine all possible ways EFDS could be accessed and if a working audit trail existed which could identify improper accesses to the taxpayer data.
2. Determined if the audit trail information was valid and reliable.
- a) Accessed 155 records from the various files available on EFDS and compared the accesses back to the audit trail reports. These records were selected from all EFDS host sites (Andover, Austin, Cincinnati, Memphis, and Ogden Service Centers).
 - b) Determined if audit trail report information was incorrect when it showed employees were accessing taxpayer accounts during their off-duty hours.
3. Determined if the audit trail reports were properly reviewed on a regular basis.

Review of the Electronic Fraud Detection System

- a) Determined who was responsible for generating and reviewing EFDS audit trail reports at the Ogden and Cincinnati Service Centers.
 - b) Interviewed those with responsibility over reviewing audit trail reports to determine how often they generated the audit trail reports and what information they looked for when reviewing the reports.
4. Evaluated the audit trail reports to determine if the information was meaningful and useful and whether unauthorized employee accesses could be readily identified.
- a) Reviewed the information contained on the EFDS Return and Document Locator Number audit trail reports to determine if enough information was available to make the reports meaningful.
 - b) Had three auditors in the Ogden Service Center access their own accounts to determine whether these accesses would be easily identified on the audit trail reports.

III. We determined if vendor contracts addressed user needs and whether the Project Office maintained reliable project cost data.

- A. Determined if vendor contracts were complete and reasonable and addressed user needs.
- 1. Evaluated current vendor contracts for content and reasonableness, including:
 - a) Whether the contracts addressed the Internal Revenue Service's EFDS Business Case goals and objectives.
 - b) Whether the contracts contained a list of deliverables and delivery dates, along with recourse if the vendor failed to meet delivery dates or acceptance criteria.
 - c) Whether the contracts included specifications for performance, functionality, and system down times.
 - d) Whether the contracts contained maintenance agreements.
 - e) Whether the contracts contained requirements for on-site support (time requirements, competency of personnel assigned, background investigations, etc.).
 - 2. Determined why some of the program applications had not been implemented as planned.
 - a) Interviewed Project Office personnel to determine the current functionality of the system.

Review of the Electronic Fraud Detection System

- b) Reviewed system-planning documentation to determine the planned functionality of the system.
 - c) Reviewed applicable contracts to determine delivery dates for the applicable applications.
 - d) Interviewed Project Office and CID personnel to determine why the applications were not implemented and determined reasonableness of responses.
- B. Assessed the reliability of Project Office records for recording project costs.
- 1. Determined if management had performed any cost-benefit analysis for EFDS.
 - a) Interviewed Project Office personnel to determine if cost-benefit analysis had been performed.
 - b) Reviewed cost-benefit analysis contained in the most recent Business Case prepared by the Project Office.
 - 2. Determined if EFDS project costs are appropriate, properly accumulated, tracked, and controlled.
 - a) Interviewed Project Office personnel to determine how project costs are accumulated, tracked, and controlled.
 - b) Reviewed these procedures to determine if proper and reasonable.
 - c) Reviewed the Project Office records to determine if the expenditures were appropriate, and to determine the completeness and accuracy of the recorded amounts.
 - 1) Footed and cross-footed the EFDS Lifecycle Cost Figures spreadsheet, which reports project costs by Sub-Object Class (SOC) and by fiscal year.
 - 2) Traced the Fiscal Year (FY) 1997 cost figures from the EFDS Lifecycle Cost Figures spreadsheet to each SOC detailed ledger.
 - 3) Reconciled the SOC detailed ledgers' individual and collective beginning balances to EFDS' FY 1997 appropriation.
 - 4) Footed each SOC detailed ledger.
 - 5) Selected a sample of entries from each SOC detailed ledger and traced to supporting documentation (timecards, travel vouchers, training requests, invoices, etc.).

Review of the Electronic Fraud Detection System

- 6) For each SOC, traced a sample of supporting documents to the SOC detailed ledger to determine the completeness of the recorded amounts.
 - 7) Traced all transfers among the SOC detailed ledgers to supporting documentation.
 - 8) Determined if the Project Office reconciles its project cost data with the Project Cost Accounting Subsystem (PCAS) cost data maintained by the Office of the Chief Financial Officer.
 - 9) Obtained a PCAS report for FY 1997 EFDS expenditures by SOC from the Budget Execution Office and compared the individual and collective SOC expenditures listed on the report to the amounts recorded by the Project Office.
- d) From accounting records, determined the cost of the project from its inception to the current date.
- 1) Determined the cost of the project from its inception to the date the Project Office was established.
 - 2) Determined the cost of the project from the date the Project Office was established through FY 1997. Included Project Office and non-Project Office costs.
 - 3) Determined if there was a sufficient basis for the IRS to continue funding for Los Alamos National Laboratories (LANL) research and development efforts.
 - a) Interviewed Project Office and CID personnel to determine what has been delivered and what is planned for future delivery from LANL.
 - b) Reviewed present and future spending for the LANL contract.
 - c) Reviewed decision to discontinue funding for LANL by Project Office and CID.

Major Contributors to This Report

Steve Mullins, Regional Inspector General for Audit
Mary Baker, Deputy Regional Inspector General for Audit
Kyle Andersen, Audit Manager
Larry Madsen, Senior Auditor
Jeff Anderson, Auditor
Roy Thompson, Auditor
Nancy Prather, Auditor
Mike VanNevel, Auditor
Doug Barneck, Auditor

**Review of the
Electronic Fraud Detection System**

Appendix III

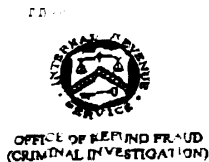
Report Distribution List

Chief Information Officer IS
Deputy Chief Information Officer, Systems IS
Assistant Commissioner for Systems Development IS:S
Assistant Commissioner for Service Center Operations IS:SC
Director, Office of Information Resources Management IS:IR
Director, Office of Systems Standards and Evaluation IS:E
Director, Office of Security Standards and Evaluation IS:E:S
Chief, Information Systems Audit Assessment and Control Section IS:I:IS:O:A
Audit Liaison, Information Systems IS:I:IS:O:A
EFDS Project Manager IS:AD:SP:E:EFDS
Assistant Commissioner (Criminal Investigation) OP:CI
National Director, Tax Refund Fraud OP:CI:ORF
National Director for Legislative Affairs CL:LA
Office of Management Controls M:CFO:A:M

**Review of the
Electronic Fraud Detection System**

Appendix IV

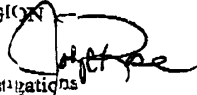
**Response from Director of Investigations, Office of Refund Fraud,
to Audit Memorandum**



DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

July 1, 1998

MEMORANDUM FOR REGIONAL INSPECTOR
WESTERN REGION

FROM: Johnny C. Rose 
Director of Investigations
(Tax Refund Fraud) OP: CI:ORF

SUBJECT: Interim Results of Electronic Fraud Detection System (EFDS)
Security Controls Testing—Urmem 6/4/98

We concur with your recommendation to reemphasize security procedures contained in the EFDS Account and User Policy and that operational reviews of the Criminal Investigation Branches (CIB) should ensure that these policies are being followed. We have taken the following actions:

1) On May 21, 1998, we sent a copy of the document to all Chiefs with instructions to review it and ensure that everyone was in compliance with it. They were also advised that this would be an item in upcoming operational reviews.

2) On May 20, 1998, we notified the CI Review and Program Evaluation to include this item in operational reviews of the service centers.

3) On June 30, 1998, we again sent the information to the Chiefs.

My office participates in each of the Operational Reviews and will determine compliance with these procedures. Any deficiencies found will be addressed with Service Center management in the prescribed manner. Copies of the correspondence regarding this issue is attached. If there are any questions, please feel free to contact Pam Hush of my staff at (202) 622-5218.

Attachments (3)

**Effectiveness of the
Electronic Fraud Detection System**

Appendix V

Management's Response to the Draft Report



DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

FEB 8 1999

MEMORANDUM FOR TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

FROM: *for* David W. Junkins *Mike Parker*
Director, Office of Information Resources Management IS:IR

SUBJECT: Management Response to Draft Internal Audit Report -
Effectiveness of the Electronic Fraud Detection System

The Assistant Commissioner for Systems Development (IS:S), the Assistant Commissioner for National Operations (IS:O), the Assistant Commissioner for Service Center Operations (IS:SC) and the Director, Security Standards and Evaluation (IS:E:S) have reviewed the subject Draft Internal Audit Report, and are providing the attached management response.

If you have any questions, please call me on (202) 283-4060 or have a member of your staff call Donna Downing on (202) 283-4159.

Attachment

cc: Regional Inspector - Western Region
Assistant Inspector General for Audit
Director, Audit Projects

**Effectiveness of the
Electronic Fraud Detection System**

The Office of Refund Fraud has Freedom of Information Act (FOIA) issues with the disclosure of any EFDS information as it is protected under "Orange Cover Security."

Recommendation # 1

The EFDS project office should work with EFDS developers to ensure that the following programming changes are made:

2b, 2e-----

Assessment of Cause

2b, 2e-----

Corrective Actions # 1A and 1B

- A) Password assignment is spelled out in the COH. The SA/Database Administrator (DBA) at the field sites have removed the old file "create_users_sh." Step four on page 7 of transmittal 98spe-013A-EFDS has been eliminated.
- B) For Processing Year (PY) 1999, the EFDS operating system for the workstation platform has been converted to 2b, 2e----- At this point, 2b, 2e-----

2b, 2e-----
2b, 2e----- The EFDS application resides on the 2b, 2e-----

Implementation Date for Corrective Action # 1A

Completed: ____ 07/17/98____

Remove file "create_users_sh"

**Effectiveness of the
Electronic Fraud Detection System**

Implementation Date for Corrective Action # 1B

Completed: __01/19/99__

Proposed:

Implemented programming
changes after conversion to
2b, 2e-----

Responsible Official for Corrective Action # 1

Chief Information Officer IS

Deputy Chief Information Officer (Systems) IS

Assistant Commissioner for Systems Development IS:S

Director, Submission Processing Division IS:S:SP

Recommendation # 2

2b, 2e-----

Assessment of Cause

The Project Office had no direct way to programmatically enforce this issue through either 2b, 2e----- Passwords for the application are 2b, 2e passwords, and without the purchase of an additional software tool, 2b, 2e 2b, 2e----- the EFDS application is not capable of retrieving this information from 2b, 2e---proprietary software. EFDS has provided the means to perform this function through contractor written subroutines, however.

Corrective Action # 2

2b, 2e-----

For PY 1999, the EFDS operating system for the workstation platform has been converted to 2b, 2e----- At this point, 2b, 2e-----
2b, 2e-----

2b, 2e----- The EFDS application resides on
the 2b,workstations. 2b, 2e-----
2b, 2e-----

**Effectiveness of the
Electronic Fraud Detection System**

Implementation Date for Corrective Action # 2

Completed: _____

Proposed: 07/01/99

Work with IS:PM to review,
evaluate, and assist in the
purchase of 2b,

Proposed: 04/01/2000

Implement 2b,

Responsible Official for Corrective Action # 2

Chief Information Officer IS

Deputy Chief Information Officer (Systems) IS

Assistant Commissioner for Systems Development IS:S

Director, Submission Processing Division IS:S:SP

Recommendation # 3

2b, 2e-----

Assessment of Cause

2b, 2e-----

Corrective Action # 3

For PY99, the EFDS workstation platform has been converted to 2b, 2e-----
operating system. At this point, 2b, 2e-----
2b, 2e-----

2b, 2e-----

However, the EFDS Contractor shall continue to support the IRS standards for
the application.

2b, 2e-----

**Effectiveness of the
Electronic Fraud Detection System**

2b, 2e-----

Implementation Date for Corrective Action # 3

Completed: _____

Proposed: 07/01/99

Work with IS:PM to review,
evaluate, and assist in the
purchase of 2b,

Proposed: 04/01/2000

Implement 2b,

Responsible Official for Corrective Action # 3

Chief Information Officer IS

Deputy Chief Information Officer (Systems) IS

Assistant Commissioner for Systems Development IS:S

Director, Submission Processing Division IS:S:SP

Recommendation # 4

2b, 2e-----

Assessment of Cause

2b, 2e-----

Corrective Action # 4

2b, 2e-----

2b, 2e-----

**Effectiveness of the
Electronic Fraud Detection System**

Implementation Date for Corrective Action # 4

Completed: _____

Proposed: 07/01/99

Work with IS:PM to review,
evaluate, and assist in the
purchase of 2b,

Proposed: 04/01/2000

Implement 2b,

Responsible Official for Corrective Action # 4

Chief Information Officer IS

Deputy Chief Information Officer (Systems) IS

Assistant Commissioner for Systems Development IS:S

Director, Submission Processing Division IS:S:SP

Recommendation # 5

2b, 2e-----

Assessment of Cause

The requirements as defined for the audit trail overlook some of these issues and need to be resolved. However, conversion to 2b, 2e-----and the accelerated time frame for Year 2000 deliverables preclude immediate corrective action with current funding.

Corrective Action # 5

The EFDS Project Office has requested the Assistant Commissioner for Program Management and Architecture, IS:PM, to review, evaluate and assist in formulating a plan for the interface between EFDS and Audit Trail Lead Analysis System (ATLAS) 2b, 2e-----
2b, 2e----- The EFDS Project Office will use IRM 2.1.10 as the basis for the overall design of the audit trail.

2b, 2e----- The EFDS
Project Office has modified the SOW to include this task.

**Effectiveness of the
Electronic Fraud Detection System**

Implementation Date for Corrective Action # 5

Completed: _____

Proposed: 07/01/99

Formulate Plan to 2b, 2e-----
2b, 2e-----

Proposed: 04/01/2000

Implement EFDS audit trail plan.

Responsible Official for Corrective Action # 5

Chief Information Officer IS

Deputy Chief Information Officer (Systems) IS

Assistant Commissioner for Systems Development IS:S

Director, Submission Processing Division IS:S:SP

Recommendation # 6

2b, 2e-----

Assessment of Cause

The requirements as defined for the audit trail overlook some of these issues and need to be resolved. However, conversion to 2b, 2e-----and the accelerated time frame for Year 2000 deliverables preclude immediate corrective action with current funding.

Corrective Action # 6

The EFDS Project Office has requested the Assistant Commissioner for Program Management and Architecture, IS:PM, review, evaluate and assist in formulating a plan for the interface between EFDS and ATLAS that will address the implementation of the recommended 2b, 2e-----

2b, 2e-----

2b, 2e----- An initial meeting was held on October 22, 1998, which included the necessary partners. Another meeting was held on November 5, 1998, with IS:PM to further discuss their support of this effort. The EFDS Project Office will use IRM 2.1.10 as the basis for the overall design of the audit trail and has modified the SOW to include this task.

**Effectiveness of the
Electronic Fraud Detection System**

Implementation Date for Corrective Action # 6

Completed: _____

Proposed: 07/01/99

Formulate Plan to 2b, 2e-----
2b, 2e-----

Proposed: 04/01/2000

Implement EFDS Interface Plan.

Responsible Official for Corrective Action # 6

Chief Information Officer IS

Deputy Chief Information Officer (Systems) IS

Assistant Commissioner for Systems Development IS:S

Director, Submission Processing Division IS:S:SP

Recommendation # 7

Determine why the EFDS application audit trail is recording inaccurate or unnecessary entries. Reprogram the audit report segments of the system to accurately reflect user actions on the system.

Assessment of Cause

The inaccurate entries situation was found during the audit review and subsequently reported as a critical National Office Command Center (NOCC) problem in 1998.

Corrective Action # 7

All programming issues relating to the recording of inaccurate or unnecessary entries have been corrected with transmittal # 25R3 dated March 16, 1998, at the field sites.

Implementation Date for Corrective Action # 7

Completed: 03/16/98

Proposed:

Correct inaccurate and
unnecessary entries on audit
trail.

**Effectiveness of the
Electronic Fraud Detection System**

Responsible Official for Corrective Action # 7

Chief Information Officer IS

Deputy Chief Information Officer (Systems) IS

Assistant Commissioner for Systems Development IS:S

Director, Submission Processing Division IS:S:SP

Recommendation # 8

The EFDS Project Office should work with EFDS developers to ensure that the following programming changes are made:

A. The EFDS application audit reports 2b, 2e-----

B. Adequate file space should also be allocated to assure available space to generate the reports.

Assessment of Cause

A. The requirement to segment the data by 2b, 2e----- had not been established in IRM 2.1.10 for the current system. In addition, conversion to 2b, 2e-----and the accelerated time frame for Year 2000 deliverables preclude immediate corrective action with current funding.

B. This program problem was found as a result of the Internal Audit review.

Corrective Action # 8

A. The EFDS Project Office will request the Assistant Commissioner for Program Management and Architecture, IS:PM, review, evaluate and assist in formulating a plan for the interface between EFDS and ATLAS that will address the implementation of the recommended design to include a 2b, 2e-----
2b, 2e----- Also, assist in developing the EFDS audit trail design to 2b, 2e-----

B. For Processing Year (PY) 1999, the system has been sized to accommodate report generation.

Implementation Dates for Corrective Actions # 8A and 8B

A. Completed: _____

Proposed: 07/01/99

Formulate Plan to 2b-----

2b, 2e-----

**Effectiveness of the
Electronic Fraud Detection System**

Proposed: 04/01/2000

Implement EFDS audit trail plan.

B. Completed: 01/19/99

Proposed:

System size was
increased to
accommodate report
generation.

Responsible Official for Corrective Action # 8

Chief Information Officer IS

Deputy Chief Information Officer (Systems) IS

Assistant Commissioner for Systems Development IS:S

Director, Submission Processing Division IS:S:SP

Recommendation # 9

A) A memorandum of understanding regarding controlling unauthorized accesses to taxpayer information was signed by IRS Executives in August and September 1997. The memorandum of understanding calls for the Chief Information Officer to: ensure that all IRS information systems contain suitable and operational audit trails; and to assess the systems that process and contain taxpayer data to determine which systems have audit trails, and how those audit trails work. The assessment should contain recommendations to improve the use of specific audit trails. The assessment was to be provided to certain executives including the Chief Inspector. A staff member of the Chief Inspector's Centralized Case Development Center informed us that they have not received an assessment for EFDS.

B) The Chief Information Officer should complete this assessment, taking into consideration the audit trail issues referred to in this memorandum to improve the usefulness of the EFDS application audit trail. Consideration should be given to audit trail elements that will be 2b, 2e-----

2b, 2e-----

The Chief Inspector's Centralized Case Development Center will assist the Chief Information Officer's staff in developing specific audit trail requirements necessary for use in a Post Audit Analysis System, such as recording of significant events, capturing ample information, and accessing the event information.

Effectiveness of the Electronic Fraud Detection System

Assessment of Cause

Neither specific guidance nor requirements have been established in IRM 2.1.10 2b, 2e-----for Tier 2 systems. Currently, EFDS does not have access to employee information.

Corrective Actions # 9

A) The IRS' Security Infrastructure Implementation Plan (120 Day Report), dated November 7, 1997, responded to the Memorandum of Understanding. It identified system capabilities, deficiencies, and enhancements planned. For EFDS, it noted that automated analysis tools are not available but that this would be enhanced with the deployment of future architecture. In this regard, it also noted that the Interim Regional Infrastructure System (IRIS) is intended to audit all events and will forward this information to an authoritative data repository and analysis system. IRIS is scheduled to be deployed as part of Phase 1, Sub-release 1.3 of the Modernization Blueprint Sequencing Plan. The IRS' Security Infrastructure Implementation Plan requires protection and, therefore, had a limited distribution which included the Deputy, Chief Inspector. More specific information can be obtained from Tim Schmidt, Director, Strategic Project Office, IS:O:SP, at 202-283-5722.

B) A conference call was held on August 13, 1998, between the EFDS Project Office, the EFDS programming contractor and the Centralized Case Development Center (CCDC). Issues discussed include data form requirements, file and record layout, media transfer type, code to application mapping, five year repository of audit trail data on EFDS and the possible use of the software package, 2b, 2 Information exchange included the EFDS database specifications to CCDC and the ATLAS record format to EFDS. EFDS is prepared to furnish whatever information is required after being given the audit program record requirements and examining methods for file transfer program retrieval by CCDC. 2b, 2e-----
2b, 2until needed for review as CCDC does not have provisions to accept the audit trail data from mini systems. A subsequent meeting was held on October 22, 1998, by the EFDS Project Office to further develop CCDC audit trail data requirements with the assistance of the Assistant Commissioner for Program Management and Architecture.

Implementation Date for Corrective Action # 9A

Completed: 11/07/97

**Effectiveness of the
Electronic Fraud Detection System**

Implementation Date for Corrective Action # 9B

Completed: _____

Proposed: 07/01/99

Formulate Plan to 2b, 2e-----
2b, 2e-----

Proposed: 04/01/2000

Implement EFDS audit trail plan.

Responsible Official for Corrective Action # 9

Chief Information Officer IS

Deputy Chief Information Officer (Systems) IS

Assistant Commissioner for Systems Development IS:S

Director, Submission Processing Division IS:S:SP

Recommendation # 10

Because of the sensitivity of the data maintained on EFDS, and the number of people who have access to the system (with more planned in the future), the audit trail problems referred to in the report should be included by the IRS as a Federal Manager's Financial Integrity Action (FMFIA) material weakness.

Assessment of Cause

Findings: Access controls should be improved. 2b, 2e-----
2b, 2e-----

The requirements as defined for the audit trail overlook some of these issues and need to be resolved. However, conversion to 2b, 2e-----and the accelerated time frame for Year 2000 deliverables preclude immediate corrective action with current funding.

The requirement to segment the data by 2b, 2e----- had not been established in IRM 2.1.10 for the current system. These situations were found during the audit review and subsequently reported as a critical NOCC in 1998.

**Effectiveness of the
Electronic Fraud Detection System**

Corrective Action # 10

The EFDS Project Office has requested the Assistant Commissioner for Program Management and Architecture, IS:PM, to review, evaluate and assist in formulating a plan for the interface between EFDS and ATLAS 2b, 2e-----
2b, 2e-----

2b, 2e----- The EFDS Project Office has modified the SOW to include this task. A meeting was held on October 22, 1998, which included the necessary partners, in an attempt to formulate an implementation plan.

All programming issues relating to the recording of inaccurate or unnecessary entries have been corrected with transmittal # 25R3 dated March 16, 1998, at the field sites.

Audit trail weaknesses are currently included in the FMFIA material weakness for Service Center security, which is being addressed in the security plans currently being overseen by the Security Standards and Evaluation Office.

Implementation Date for Corrective Action # 10

Completed: _____

Proposed: __07/01/99__

Formulate Plan to 2b, 2e-----
2b, 2e-----

Proposed: __04/01/2000

Implement EFDS audit trail plan.

Responsible Official for Corrective Action # 10

Chief Information Officer IS

Deputy Chief Information Officer (Systems) IS

Assistant Commissioner for Systems Development IS:S

Director, Submission Processing Division IS:S:SP

Effectiveness of the Electronic Fraud Detection System

Recommendation # 11

Information Systems should clearly define in IRS IRMs or other policy statements who is responsible for performing security reviews on systems such as EFDS and ensure that these reviews are performed.

Assessment of Cause

Interviews with Information Systems (IS) security functions at six service centers to determine if their offices had ever performed any security reviews pertaining to EFDS resulted in only one site stating that they had performed a security review. Reasons given for not performing the reviews included lack of resources and questions as to who was responsible for performing the EFDS reviews.

Corrective Action # 11

IRM 2.1.10, Information Systems Security, Section 10.4, Security Guidelines Overview, provides information systems security guidelines, including individual duties and responsibilities for security reviews. The IS Security and Certification Program Office has the responsibility for ensuring that this IRM is updated and current.

The IRS' Office of Security Standards and Evaluation will perform management reviews to ensure that security reviews of EFDS and other sensitive systems are performed. This activity is part of our ongoing reviews, with EFDS being reviewed at each site we visit.

Implementation Date for Corrective Action # 11

Completed: ____12/01/98____

Proposed:

IRM 2.1.10 defines security reviews
and responsibilities.

Responsible Official for Corrective Action # 11

Chief Information Officer IS

Deputy Chief Information Officer (Operations) IS

Assistant Commissioner for National Operations IS:O

Director, Telecommunications and Operations Division IS:O:O

Director, Systems Standards and Evaluation IS:E

Recommendation # 12

The EFDS Project Office should review the current C2 required documentation and update the information to reflect the current programming and operating procedures of EFDS.

Effectiveness of the Electronic Fraud Detection System

Assessment of Cause

The C2 documentation was written by the Security contractor under our original security certification in 1996. Rapid progress and extensive system enhancements to EFDS postponed updating the C2 documentation. However, the current system security features are discussed during the SA/DBA and the Criminal Investigation Division (CI) end-user annual training.

Corrective Action # 12

C2 re-certification began in May 1998. We will update all of our C2 documents according to guidelines. We have secured the contractor to assist us in performing this task.

Implementation Date for Corrective Action # 12

Completed: _____

Proposed: 08/01/99

Update C2 documentation.

Responsible Official for Corrective Action # 12

Chief Information Officer IS

Deputy Chief Information Officer (Systems) IS

Assistant Commissioner for Systems Development IS:S

Director, Submission Processing Division IS:S:SP

Recommendation # 13

We were informed that EFDS will soon undergo a new security certification. In our opinion, taking into account the audit trail and documentation issues discussed in this report, it is questionable whether EFDS should have received its prior security certification. In the upcoming certification process, Information Systems should ensure that the issues discussed in this report are corrected, and that all other controls necessary for a proper certification are in place and functioning.

Assessment of Cause

EFDS is required to meet C2 security criteria which requires the following documentation: Security Features User's Guide, Trusted Facility Manual, Security Test and Evaluation Report, and Design Documentation. In reviewing the C2 documentation there were statements referring to security features that are not in place on EFDS such as 2b, 2e-----
2b, 2e----- In addition, there was a lack of references to security features that should be addressed in the documentation such as application audit trail procedures. Throughout the

Effectiveness of the Electronic Fraud Detection System

documents, there are also references to the 2b, 2operating system. Because EFDS will be converting over to the 2b, 2e-----operating system, references in the documentation to the 2b, 2system will also become outdated.

The EFDS Security Features User's Guide contains the following statement "through understanding implemented security mechanisms, users are able to consistently and effectively protect IRS-maintained information." However, if the information found in the C2 documentation is not accurate or does not reflect current system programming, users could rely on controls which are not functioning and compromise the security of the system.

Corrective Action # 13

The EFDS Project Office has begun the new security certification process. A Statement of Work (SOW) was prepared for a contractor to perform the security certification. Currently, the contract costs are being negotiated and work is expected to begin soon. The Project Office will ensure issues are corrected and all other controls for certification are in place. A copy of this Internal Audit report has also been shared with the IS Certification Program Section (IS:O:O:S:C) to ensure all issues are corrected and that all other controls necessary for certification are in place and functioning.

Implementation Date for Corrective Action # 13

Completed: _____

Proposed: 10/01/99

Obtain C2 certification of EFDS.

Responsible Official for Corrective Action # 13

Chief Information Officer IS

Deputy Chief Information Officer (Systems) IS

Assistant Commissioner for Systems Development IS:S

Director, Submission Processing Division IS:S:SP

Recommendation # 14

The EFDS Project Office should ensure that EFDS Contingency Plans are updated and tested at least annually. In addition, the plan should be made available to all concerned parties (system administrators, Criminal Investigation Division system users, etc.)

Assessment of Cause

The documents were not updated due to numerous program and system enhancements over the past few years. However, contingency plans were

**Effectiveness of the
Electronic Fraud Detection System**

known and shared with the SA/DBA and the end user. The final contingency is the use of the paper system.

Corrective Action # 14

The Contingency Plan will be updated to reflect the PY 1999 system. Each site is required to backup the EFDS data and contingency testing is scheduled locally. Each site SA/DBA has also been provided training at the annual SA/DBA training session to allow them to perform backup and recovery processes for a number of items which could occur in a normal production environment.

Implementation Date for Corrective Action # 14

Completed: _____

Proposed: 05/01/99

Update EFDS Contingency
Plans.

Responsible Official for Corrective Action # 14

Chief Information Officer IS

Deputy Chief Information Officer (Systems) IS

Assistant Commissioner for Systems Development IS:S

Director, Submission Processing Division IS:S:SP

Recommendation # 15

The EFDS Project Office should ensure that program changes are made to EFDS which would allow returns with the highest fraud potential to be worked first.

Assessment of Cause

This is a new problem that was found during the audit. This problem was not detected by Product Assurance during Systems Acceptability Testing (SAT) 1997, nor has it been reported by the end user, Criminal Investigation Division, during PY 1998.

Corrective Action # 15

The changed application which allows priority returns with the highest fraud potential to be worked first was corrected for PY 1999.

Implementation Date for Corrective Action # 15

Completed: 01/19/99

Proposed:

Implemented change to allow
priority returns to be worked first.

**Effectiveness of the
Electronic Fraud Detection System**

Responsible Official for Corrective Action # 15

Chief Information Officer IS

Deputy Chief Information Officer (Systems) IS

Assistant Commissioner for Systems Development IS:S

Director, Submission Processing Division IS:S:SP

Recommendation # 16

The Project Office and Criminal Investigation Division should reach agreement regarding what constitutes a definitive functional requirements package. When the functional requirements are delivered, the Project Office should give timely, complete, and detailed feedback regarding changes necessary to the functional requirements.

Assessment of Cause

The events described in the memorandum pre-date the Project Office's requirement of written functional requirements from the customer. Since that time, we have notified the customer in extensive joint meetings what items would be accomplished as well as the timeframes. This is only the first step in a very long process toward the Capability Maturity Model and requires all EFDS Project Partners commitment and agreement to the processes.

Corrective Action # 16

System Development Life Cycle meetings along with the appropriate walk throughs have been ongoing between EFDS Partners since August 1997. The EFDS Project Office is in the process of implementing Configuration Control Board (CCB) and Requirements Traceability (RT) within the Project. This requires all partners to agree to the requirements before they are forwarded for approval. The processes for RT need to be defined and implemented to assist the CCB in making informed decisions on requirements and changes within the system.

Implementation Date for Corrective Action # 16

Completed: ____08/97____

Proposed: _____

Reach agreement on functional
requirements package.

Responsible Official for Corrective Action # 16

Chief Information Officer IS

Deputy Chief Information Officer (Systems) IS

Assistant Commissioner for Systems Development IS:S

**Effectiveness of the
Electronic Fraud Detection System**

Director, Submission Processing Division IS:S:SP

Recommendation # 17

Utilizing the information developed by Internal Audit as a starting point, the Project Office should make a thorough review of EFDS cost records to ensure that no other misstatements or omissions have occurred. The Project Office should maintain a schedule of non-Project Office and Project Office costs. The non-Project Office costs should include those costs identified in this review plus any other identifiable costs. The Project Office should maintain supporting documentation for each of these amounts. The Project Office costs should include costs for each EFDS Project Cost Accounting System (PCAS) code since Fiscal Year 1995 when the Project Office was established. Each PCAS code amount should be supported by an Automated Financial System (AFS) report containing most current actual data. The sum of these two amounts is the total EFDS project cost. This is the amount that the Project Office should use when preparing reports for or providing cost data to users outside of the Project Office.

Assessment of Cause

For fiscal year 1994, (pre-Project Office) hardware and software was acquired through multiple sources. Therefore, historical documents were not centrally maintained. The Project Office requested and received all known historical documents in an effort to preserve this information. For fiscal year 1995 and fiscal year 1996, the financial process had been very volatile. Continuing Resolutions, No-Year funds, purchasing through the "exception" rule, all attributed to the inability to reconcile all monies to the then established PCAS codes.

Corrective Action # 17

We will begin with the historical information already sorted via this investigation and use IRS mandated systems to continue to track costs.

Implementation Date for Corrective Action # 17

Completed: _____

Proposed: 04/01/99

Track project and non-project costs and maintain documentation.

**Effectiveness of the
Electronic Fraud Detection System**

Responsible Official for Corrective Action # 17

Chief Information Officer IS
Deputy Chief Information Officer (Systems) IS
Assistant Commissioner for Systems Development IS:S
Director, Submission Processing Division IS:S:SP

Recommendation # 18

The Project Office should reconcile their cost data to source documentation and to AFS on a regular basis. The amount recorded should be changed if the purchase order or the expenditure amounts differ from the requisition amount. Reconciled Project Office cost data should be archived at the end of each fiscal year for future reference.

Assessment of Cause

EFDS has made an effort to maintain accurate and appropriate cost records. Discrepancy reports were submitted to the AFS organization, however, fiscal year closure prohibited its update.

Corrective Action # 18

The Project Office currently reconciles costs monthly between AFS and our source documentation. Reconciled Project Office cost data is archived at the end of each fiscal year.

Implementation Date for Corrective Action # 18

Completed: ____10/23/98____

Proposed:

Reconcile costs monthly and
archive data fiscally.

Responsible Official for Corrective Action # 18

Chief Information Officer IS
Deputy Chief Information Officer (Systems) IS
Assistant Commissioner for Systems Development IS:S
Director, Submission Processing Division IS:S:SP

Description of C2-Level Security

The Department of Defense has developed a multi-level system for classifying computer system security, commonly known as the Orange Book. The classification system ranges from class D (Minimal Protection) to class A1 (Verified Design). The Department of the Treasury requires that its automated information systems "processing, storing, or transmitting sensitive but unclassified data will meet the requirements for a C2 level of protection (Controlled Access Protection)."

Systems in the C2 class enforce a finely grained discretionary access control mechanism, making users individually accountable for their actions. This accountability is achieved through login procedures, auditing of security-relevant events, and resource isolation. Systems in this class are required to achieve a minimum level of assurance through requirements for system architecture, system integrity, and security testing. Federal agencies operating Class C2 systems are also required to maintain documentation covering the security features of the system as well as testing and design documentation.

The risk of not meeting one or more of the C2-level requirements can lead to the opening of security exposures in the system. For example, if a system does not meet the Object Reuse requirement (resource isolation), it runs the risk of having deleted data retrieved without the owner's consent. The Object Reuse section requires that the system assure that a storage object (e.g., disk file, etc.) has been cleared before it is initially assigned, allocated, or reallocated to a system user. Failure to clear the object before assignment allows the newly assigned user the opportunity to retrieve deleted data from the object.

Glossary of Terms Used in This Report

Access	The ability and the means to approach, view, store or retrieve data, to communicate with, or to make use of any resource of an information system.
Access Controls	Methods used to limit access to the resources of an information system (hardware, software, data) thereby restricting and controlling system use only to authorized users, programs, processes, and network systems to access ports and other information.
Application	A specific task-oriented program, such as the Electronic Fraud Detection System (EFDS), supplied or designed to suit individual user needs.
Application Audit Trail	An audit trail which is specific to an application. EFDS has four application audit trail reports which include the Program Audit Trail Report, the Return Audit Trail Report, the W-2 Audit Trail Report, and the Document Locator Number (DLN) Audit Trail Report.
Audit Trail	A chronological record of system activities that is sufficient to permit reconstruction, review, and examination of the sequence of environments and activities surrounding or leading to each event in the path of a transaction, from its inception to final results.
Automated Financial System	A computer based financial accounting system used by the Internal Revenue Service (IRS) to track appropriations and expenditures.

Effectiveness of the Electronic Fraud Detection System

Controlled Access Protection (C2)	A level of protection used to deny unauthorized access to an information system that can be accessed by more than one user. With controlled access protection, users do not have the same authorization level to access, store, or process data. See Appendix VI for further information regarding C2 Security.
Data Base	A structured collection of largely unique data items or records maintained in one or more computer files, which may be processed by one or more systems.
Data Base Administrator (DBA)	The person responsible for maintaining and updating EFDS database files.
DLN Audit Trail Report	This EFDS audit trail report tracks changes in a particular DLN through the system, recording actions taken by EFDS users on the return and associated Forms W-2. (Form W-2 reflects a taxpayers' wages earned and federal income tax withheld).
Document Locator Number (DLN)	The DLN is a number assigned to every tax return to assist in controlling, identifying and locating the return.
Federal Managers Financial Integrity Act (FMFIA)	Legislation requiring federal agencies to establish and maintain adequate internal control systems. The Act also requires an annual report documenting agency compliance/noncompliance with internal accounting and administrative systems, and corrective actions planned when an area of noncompliance is deemed a "material weakness."
Integrated Data Retrieval System (IDRS)	IRS computer system that enables employees to have instantaneous visual access to certain taxpayer accounts.

Effectiveness of the Electronic Fraud Detection System

Operating System	An organized collection of techniques, procedures, programs, or routines for operating an information system, usually supplied by the system hardware vendor.
2b, 2e	----- -----
Password	A series of numbers or letters used by an individual to gain access to a system. A protected or private character string used to authenticate an identity.
Program Audit Trail Report	This EFDS audit trail report tracks the time an EFDS user logs on or off the system, the time of each program initiation, external database use, and workstation identification.
Questionable Refund Program (QRP)	IRS program responsible for identifying fraudulent refund returns and other noncompliance issues with an emphasis on preventing the issuance of refunds to filers of fraudulent returns.
Return Audit Trail Report	This EFDS audit trail report tracks actions taken by EFDS users on all returns. It is intended to provide the history of all DLNs through the system.
Security Certification	An independent technical evaluation for the purpose of accreditation which uses security requirements as the criteria for the evaluation.
Senior Council for Management Controls (SCMC)	The SCMC was established in December 1992 to provide agency policy, guidance, and oversight in implementing the FMFIA.

**Effectiveness of the
Electronic Fraud Detection System**

System Administrator (SA)	The person responsible for maintaining the entire EFDS computer system.
System Audit Trail	An audit trail which is specific to an operating system. In the case of EFDS, an audit trail specific to the 2b, operating system.
2b, 2e----- -----	----- ----- -----
-----	----- ----- ----- -----
User ID	A unique character string that identifies a terminal user to the system.
W-2 Audit Trail Report	This EFDS audit trail report tracks actions taken by EFDS users to verify certain entries on a taxpayer's Form W-2.